(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 195 679 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
10.04.2002 Bulletin 2002/15

(51) Int Cl.[7]: **G06F 11/14**

(21) Application number: **00308840.8**

(22) Date of filing: **06.10.2000**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(71) Applicant: **Hewlett-Packard Company,**
A Delaware Corporation
Palo Alto, CA 94304 (US)

(72) Inventor: **Gold, Stephen**
Winterbourne Down, Bristol BS36 1DJ (GB)

(74) Representative:
Lawman, Matthew John Mitchell et al
Hewlett-Packard Limited,
IP Section,
Building 3,
Filton Road
Stoke Gifford, Bristol BS34 8QZ (GB)

(54) Performing operating system recovery from external back-up media in a headless computer entity

(57) A computer entity, particularly but not exclusively a headless computer entity, has operating systems stored on a non-volatile data storage device e.g. a hard disk drive, and has a back-up data storage device. Operating system back-up's are taken from an uncorrupted copy of an operating system stored in a separate partition on the data storage device to the primary operating system which is actually used to run the device, thereby ensuring that if the primary operating system of the computer entity becomes corrupted either gradually or catastrophically, the back-up copy which is stored on a back-up media is not effected. Under failure conditions of the computer entity, a pristine copy of the operating system can be reloaded from the back-up tape data storage media and the computer entity rebooted from the pristine operating system back-up copy.

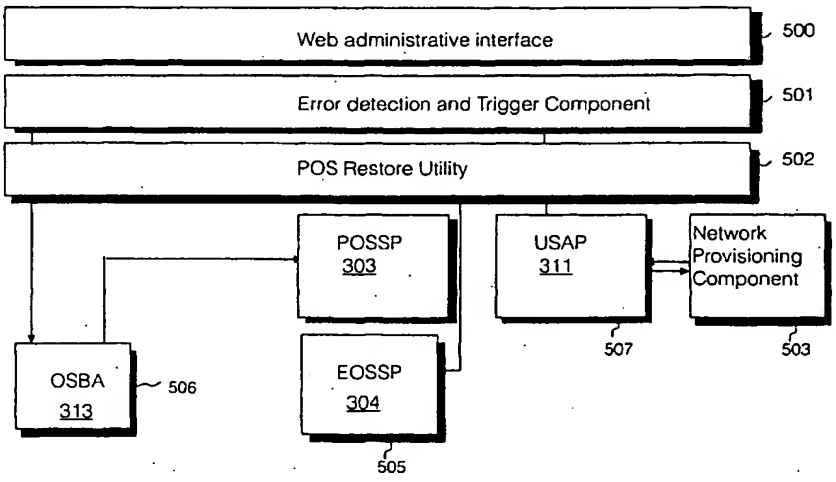

Fig. 5

EP 1 195 679 A1

Description

Field of the Invention

[0001] The present invention relates to the field of computers, particularly although not exclusively, to a method for implementing back-up of an operating system to a computer entity.

Background to the Invention

[0002] Headless computer entities, also known as "headless appliances" are known in the art. A known headless computer entity comprises a data-processor, memory, a plurality on input\output ports or the like, and an operating system. Headless appliances are generally designed without user interfaces, and lack a keyboard, pointing device e.g. mouse or track ball, and visual display monitor. This has the advantages both of reducing the cost of ownership , since the cost of a user interface hardware need not be borne by the purchaser, and also inhibiting interference with the operation of the appliance.

[0003] In a headless computer entity, human administrators are conventionally allowed only very limited access to the computer entity for maintenance, or in some cases no user maintenance is permitted. To safeguard against theft or loss of the computer entity involving loss of data, optionally a computer entity may have a back-up device, for example a tape back-up device such as DDS (Digital Data Storage) format back-up device. A back-up copy of an operating system of the computer entity may be made to the tape back-up device.

[0004] In a conventional computer entity where an operating system runs from a data storage device e.g. a hard disk, having re-write capability as opposed to read only memory, then there is a potential problem with backing up an operating system of the device onto a back-up medium e.g. tape, to provide for recovery of the computer entity after an operating system malfunction of "creeping corruption" of the back-up data. In particular, where an operating system fails gradually over a period of time, and back-up copies are made onto a separate back-up data storage medium, e.g. tape, periodically throughout the gradual period of operating system failure, then the operating system which is being backed up onto the back-up data storage medium is a corrupted or gradually corrupted version of the operating system. Under conditions of operating system failure on the computer entity, the back-up copy of the operating system must be relied on to restore the corrupted operating system. However, if the operating system stored on the back-up medium is itself corrupted, or in a partially corrupted state immediately prior to failure, then there is no way of recovering the computer entity from an operating system failure using the back-up data storage media.

[0005] Whilst the above problem exists both for conventional computer entities having a visual display and keyboard user interface, and for headless computer entities having a user interface, the problem is less acute for conventional computer entities, because the operating system can be reloaded from an original CD ROM data carrier, using the user interface. However, for headless computer entities, because there is no user interface provided, the problem is more severe.

Summary of the Invention

[0006] According to a specific implementation of the present invention, there are provided at least two copies of an operating system in a computer entity stored in a partitioned re-writable data storage device. A first (primary) copy of the operating system is used to actively control the computer entity. A secondary, copy of the operating system is used to operate the computer entity under conditions of failure or maintenance of the primary operating system. A further third copy of the primary operating system is stored on an operating system back-up partition of a re-writable data storage device, for example a disk drive or RAID array. The third copy of the operating system, is maintained as a pristine uncorrupted copy of the operating system, in its original manufactured state after installation into the computer entity.

[0007] Additionally, there are stored archived application configuration settings in a separate application setting archive partition of the data storage device.

[0008] When the operating system of the computer entity is backed up to an external data storage medium, for example a tape data storage medium for back-up purposes, the third copy of the operating system is backed up. Since the third copy of the operating system is known to be pristine and uncorrupted, and is not used for running the computer entity, there is maintained on the external back-up medium, a pristine uncorrupted copy of the operating system.

[0009] Therefore, it can be guaranteed that an uncorrupted version of the operating system can be reloaded into the computer entity from the tape data storage medium after an operating system failure of the computer entity.

[0010] This back-up copy is stored in addition to the first operating system used to run the computer entity, and the third operating system stored on the operating system back-up partition of the data storage device within the computer entity.

[0011] Upon restoring an operating system from a back-up data storage medium, the operating system is restored to the operating system back-up partition of the data storage device within the computer entity, and the application configuration settings are restored to the user settings archive partition, from which they were originally loaded onto the back-up data storage medium. Rebooting the computer entity then involves rebuilding the first copy of the operating system in a first data partition of the data storage device, from the operating system back-up area of the data storage device, with appli-

cation configuration settings of the first copy operating system being rebuilt from the pristine copy application configuration settings stored in the user settings archive partition of the internal data storage device of the computer entity.

[0012] In a specific method according to the present invention to restore an operating system from the back-up media, before the pristine third copy operating system in the operating system back-up partition is overwritten, during a restore from back-up data storage medium operation, the original third copy of the operating system within the internal data storage device is first transferred from the operating system back-up partition to a "scratch" area (a reserved space partition) of the internal data storage device as a precaution against failure of the back-up operation from the back-up data storage medium. If a restore operation to restore the operating system from the back-up data storage medium to the operating system back-up partition of the internal data storage device fails, then the original third copy operating system, which was in the operating system back-up partition can be restored from the scratch area of disk to which it has been copied. Without this facility, a failure during an operating system restore operation from a back-up data storage medium could result in a corrupted third copy of the operating system, stored in the operating system back-up partition. However, with this facility, any failure during the recovery operation from the back up media can result in the computer entity restoring to a known working configuration.

[0013] The first copy of the operating system is not always overwritten during recovery from the back-up data storage medium. During a back-up operation, version checking is performed, to compare a version of operating system already stored on the internal data storage device of the computer entity, with a version of operating system stored on the back-up data storage medium. If the version on the back-up data storage medium is a same major version, but a lower minor version, then recovery from the back-up data storage medium will overwrite the third copy of the operating system stored in the operating system back-up partition. If an operating system version stored on the internal data storage device has a same major version, but a more recent minor version, then the back-up data storage medium will not restore the third copy operating system, since the third copy operating system stored in the operating system back-up partition is a more recent version than that stored on the back-up data storage medium.

[0014] According to a first aspect of the present invention there is provided a method of performing a recovery operation of an operating system for a computer entity, said computer entity comprising:

at least one data processor; and

at least one data storage device, wherein said data storage device is configured into a plurality of partition areas;

said method comprising the steps of:

copying a back-up operating system from a back-up source onto a operating system back-up area partition which is not used for direct running of an operating system by said computer entity;

copying a user settings data from said back-up source to a user settings archive partition area of said data storage device; and

resetting said computer entity.

[0015] According to a second aspect of the present invention there is provided a method of storing a back-up operating system of a computer entity to a back-up media, said computer entity comprising a pristine copy of an operating system stored in an operating system back-up area data partition of a data storage device, and a primary operating system stored in a primary operating system partition area of said data storage device;

said method comprising:

copying a plurality of operating system files in a pristine manufactured state from said operating system back up area data partition onto a back-up media; and

copying a set of configuration settings from a user settings archive partition area of said data storage device to said back-up media.

Brief Description of the Drawings

[0016] For a better understanding of the invention and to show how the same may be carried into effect, there will now be described by way of example only, specific embodiments, methods and processes according to the present invention with reference to the accompanying drawings in which:

Fig. 1 illustrates schematically an external overview of a headless computer entity;

Fig.2 illustrates schematically a hardware-firmware architecture of the headless computer entity of Fig. 1;

Fig. 3 illustrates schematically a logical architecture for storage of operating systems within an internal data storage device of the computer entity of Fig. 1;

Fig. 4 illustrates schematically a data storage device partition of the computer entity of Fig. 1;

Fig. 5 illustrates schematically logical components cooperating to perform a restore operation from a back-up data storage medium;

Fig. 6 illustrates schematically steps carried out to create a back-up of an operating system, onto a back-up media;

Fig. 7 illustrates schematically steps for initiating a recovery from a back-up data storage medium;

Fig. 8 illustrates schematically an operation carried out by the computer entity for restoring an operating system from a back-up media;

Fig. 9 illustrates schematically a procedure for alerting a user to errors in the restoration process of Fig. 8;

Fig. 10 illustrates schematically a method carried out by the computer entity for performing a reset of the computer entity, with user data being preserved;

Fig.11 illustrates schematically an overview of a process for checking a valid operating system update version on a back-up data storage medium; and

Fig. 12 illustrates schematically a sub-routine of the operating system validity check process of Fig. 11, for checking a major operating system update.

Detailed Description of the Best Mode for Carrying Out the Invention

[0017] There will now be described by way of example the best mode contemplated by the inventors for carrying out the invention. In the following description numerous specific details are set forth in order to provide a thorough understanding of the present invention. It will be apparent however, to one skilled in the art, that the present invention may be practiced without limitation to these specific details. In other instances, well known methods and structures have not been described in detail so as not to unnecessarily obscure the present invention.

[0018] Referring to Fig. 1 herein there is illustrated schematically in perspective view a headless computer entity 100 comprising: a casing 101 containing a processor, memory, one or more data storage devices and one or more communications ports connectable to a local area network 102; a relatively small display screen, for example a liquid crystal (LCD) display 103 capable of giving limited status information for operations carried out by the computer entity, for example, POWER ON mode, a STAND BY mode, or other modes of operation; a data entry means 104, for example a CD ROM drive, and a back-up data storage device port 105, for example a digital data storage (DDS) format tape streamer.

[0019] A headless computer entity is not provided with a visual display monitor, pointing device e.g. mouse, or keyboard, or other direct user interface, and therefore is difficult for a human operator to interact with directly. In operation, the headless computer entity is intended to be self-managing and self-maintaining. Typically, a headless computer entity will provide a dedicated functionality within a network environment. Examples of headless computer entities include network attached storage devices.

[0020] Referring to Fig. 2 herein, there is illustrated schematically an architecture of hardware and firmware components of the headless computer entity 200. The entity 200 comprises one or more communications ports 201; one or more data processing devices 202 as are known in the art; a memory 203 associated with the data processor(s); at least one data storage device 204, for example a hard disk data storage device, or an array of a plurality of hard disk data storage devices; an administration interface 205; a small display, e.g. a liquid crystal display device 206; a plurality of operating systems 207 as will be described herein after; and one or a plurality of application programs 208 providing functionality to the headless computer appliance.

[0021] Referring to Fig. 3 herein there is illustrated schematically an overview of operating system 207 within the computer entity. The operating system 207 is stored on a non-volatile data storage device, for example a hard disk drive, or a RAID array. The operating system 207 comprises a primary operating system 300, which controls the computer entity under normal operation; an emergency operating system 301 which controls the computer entity at times when the primary operating system 300 is incapable of running the computer entity, for example during a failure of the primary operating system 300, or during an upgrade or replacement of the primary operating system 300; and a copy of the primary operating system, comprising a copy 303 of the code files comprising the primary operating system itself, and copies 304 of default data of the primary operating system.

[0022] After a failure of the computer entity primary operating system or if the primary operating system 300 is upgraded, or restored from a back-up data storage device, the primary operating system 300 is restored directly from the copy of the primary operating system files 303 and the default data of the primary operating system 304.

[0023] Referring to Fig. 4 herein, there is illustrated schematically a format of data storage device 204, upon which operating systems 207 are stored. The data storage device is partitioned into a logical data storage area 400 which is divided into a plurality of partitioned areas of partitions and sub-partitions according to the architecture shown. A main division into a primary partition 400 and a secondary partition 402 is made. Within the primary partition are a plurality of sub partitions including

a primary operating system system partition 403 (POSSP), containing a primary operating system of the computer entity; an emergency operating system partition 404 (EOSSP) containing an emergency operating system under which the computer entity operates under conditions where the primary operating system is inactive or is deactivated; an OEM partition 405; a primary operating system boot partition 406 (POSBP), from which the primary operating system is booted or rebooted; an emergency operating system boot partition 407 (EOSBP), from which the emergency operating system is booted; a primary data partition 408 (PDP) containing an SQL data base 409, and a plurality of binary large objects 410, (BLOBs); a user settings archive partition 411 (USAP); a reserved space partition 412 (RSP) typically having a capacity of the order of 4 gigabytes or more; and an operating system back up area 413 (OSBA) containing a back up copy of the primary operating system files 414. The secondary data partition 302 comprises a plurality of binary large objects 415.

[0024] Referring to Fig. 5 herein, there is illustrated schematically an interaction between a plurality of applications 208 and the operating systems 207, for carrying out a back-up operation to back-up a primary operating system of the computer entity, and a restore from back-up data storage medium to restore an operating system of the computer entity. Applications 208 comprise a web administration interface 500 over which a user can activate back-up data storage including back-up of an operating system to a back-up data storage device; a back-up media restore utility 501 for controlling restoration of back-up data including a back-up operating system from a back-up media; a primary operating system restore utility 502 for restoring a primary operating system; and a network provisioning component 503.

[0025] In this specification the term "back-up media" is used to describe any type of back-up media which is removable from a computer entity and can be taken away from the computer entity. Examples of back-up data storage media include tape data storage devices, writable CD ROM devices, ZIP® drives, SPARC® drives, removable hard disk drives (HDD) or the like. In the specific embodiment described herein, a tape back-up data storage device is used however, it will be understood by those skilled in the art that this device could be replaced by any suitable type of back-up data storage device.

[0026] Referring to Fig. 6 herein there is illustrated schematically a back-up process for backing up the primary operating system of the computer entity onto a back-up data storage media. In step 601, a copy of primary operating system files 414 stored in the operating system back-up area 413 are transferred on to the back-up media. Because the copy of the primary operating system files 414 stored in the operating system back-up area is a pristine uncorrupted copy of the primary operating system and is different from the copy of the primary operating system stored in the primary operating system system partition 403 which is used to run the computer entity, the primary operating system files 314 in the operating system back-up area 413 are uncorrupted, irrespective of the status of the primary operating system stored in the primary operating system partition 403.

[0027] In step 602, the content of the user settings archive partition 411 is copied onto the back-up data storage media. The data in the user settings archive partition 411 comprises data which describes a way in which a user has set up the primary operating system. Therefore backing up the current data in the user settings archive partition effectively backs up the current settings of the primary operating system which is used to run the computer entity. Therefore in the back-up operation to the data storage media, there is backed up firstly a pristine copy of the primary operating system, which has not been used operationally in the computer entity and therefore remains uncorrupted, and secondly the user settings for configuring the primary operating system, which are stored in a separate partition on the internal data storage device from both the pristine copy of the operating system files 414, and from the active primary operating system stored in the primary operating system system partition 403.

[0028] In step 603, the content of the primary data partition is copied to the back-up data storage medium; and in step 604 the content of the secondary data partition, comprising a plurality of binary large objects 415 is copied to the back-up data storage media.

[0029] Each computer entity stores a license key, authorizing a number of users, outside of the data partitions used to store the primary operating system or the copy of the primary operating system in the operating system back-up area. Therefore, during a back-up operation, there is no need to back-up the license key data. Further, the license key data of high license number machine can not be backed up onto a different machine, expanding that machines licensed capabilities, and hacking of a license key on the back-up data storage medium is avoided since the license is not stored on the back-up data storage medium.

[0030] There will now be described operation of the computer entity for recovery of an operating system from a back-up data storage media. Under conditions of disaster recovery, the back-up data storage media is inserted into the back-up data storage device 105. The back-up media contains the backed up contents of the operating system back-up area 413, the user settings archive partition 411; the primary data partition 408; including the SQL database 409; binary large objects 410; and the secondary data partition 402 including further binary large objects 415. In other words, the back-up media contains user data, user settings, and a pristine copy of the primary operating system.

[0031] Under control of an operator, accessing the computer entity via web administration interface 500 and whilst running the primary operating system 300, the back-up media restoration utility 501:

- Restores a pristine copy of the operating system, the user settings, and data back onto the data storage device of the computer entity. During this operation, a previous content of the operating system back-up area 413 is copied to the reserved space partition 412 to safeguard against errors during the recovery from back-up media.

- Once the operating system, user settings and data are recovered from the back-up media, there is initiated a reset operation of the computer entity, with data preserved, under control of the user via the web administration interface 500 and effected by the primary operating system restore utility 502. During the restore operation, control of the computer entity is handed over to an emergency operating system.

[0032] During the restoration from the back-up media, checks are made to ensure that the operating system on the back-up media is compatible with the hardware of the computer entity. During the restoration from back-up media, events are copied to an alert log, if errors occur.

[0033] Referring to Fig. 7 herein, there is illustrated process steps carried out for recovering backed up data from the back-up data storage media. A user initiates the process by accessing the web administration interface from a remote computer, and by inserting the back-up data storage media into the back-up data storage device 105. The web administration interface, displays a series of prompt displays to the user and displays a dialogue box for receiving instructions from a remote user interface. In step 701, the back-up media restore utility 501 checks the back-up data storage media for a valid primary operating system version number. In step 702, the back-up media restore utility reads a list of supported hardware types from the back-up data storage media. If, in step 703 a *current hardware type* data stored on the computer entity, is not contained in a list of supported hardware types stored on the back-up data storage media, then in step 704, the back-up media restore utility generates a message to the user that the operating system stored on the back-up data storage media is incompatible with the current computer entity hardware. This may occur where, for example the computer entity has had to be replaced after theft of an original computer entity from which data was backed up onto the back-up data storage media, or where components of the computer entity have been replaced, with new components which are incompatible with the previous components of the computer entity. Provided, in step 703 that the current hardware type of the computer entity is on the list of supported hardware types stored on the data carrier, then in step 706, the back-up media restore utility 501 generates a prompt message to the user to confirm proceeding with the restore operation. This message is displayed to the user via the web administration interface 500. If the user does not confirm or cancels the restore operation in step 707 then in step 708 the back-up data restore utility exits the procedure. However, in step 709 if the user confirms proceeding with the restoration from the back-up media, the restore utility displays the name of the computer entity, and the date on which the back up media was created. This is to allow a final user confirmation that the back up media that they are using is the correct one. In step 710, the user may confirm whether the back up media is the correct one, and following a positive confirmation in step 710, via the web administration interface, then the utility proceeds to restore the operating system from the back up media in step 711.

[0034] Referring to Fig. 8 herein there is illustrated schematically main process steps in a method for restoring the operating system from the back-up media. During the recovery from back-up media operation, the primary operating system runs the recovery algorithm. The back-up utility being an application running on top of the primary operating system. In step 801, the back-up media restore utility 501 freezes any current back-up requests which may be in operation on the computer entity, to prevent any further backing up to the data partitions that are about to be overwritten by the restore process. In step 802, the back-up media restore utility closes all the data files which are currently open on the computer entity. In step 803, a current content of the operating system back-up area 813, that is the operating system 414 currently contained in the operating system back-up area are copied into the reserved space partition 412. This is to ensure that if the back-up procedure fails, and the data within the operating system back-up area 413 in corrupted, the original content of the operating system back-up area prior to restoration from back-up media, which has been stored in the reserved space partition 402 can be recovered. Therefore, effectively the position immediately prior to a failed back-up can be recovered from the pristine copy of the operating system stored in the reserved space partition 412. In step 804, the primary data partition 408 is restored for the data contained on the back-up data storage media. In step 805, the second data partition is restored from the data stored on the back-up data storage media. Steps 804 and 805 are user selectable via the web administration interface 500. A user may wish to restore only the operating system, without restoration of data on the computer entity. In step 806, the back-up media restore utility copies the operating system from the back-up data storage media onto the operating system back-up area 413 and loads the primary operating system files 414 which have been backed up onto the back-up data storage media onto the operating system back-up area 413. In step 807, the user settings are copied from the back-up data storage media to the user settings archive partition 411. In step 808, the back-up media restore utility 501 initiates a reset with data preserve process as will be described herein after, in order to reset

the computer entity from the back-up copy operating system recovered from the back-up data storage medium.

[0035] Referring to Fig. 9 herein, there is illustrated schematically a procedure which runs in parallel with the restoration procedure of Fig. 8, and is activated where an error in restoration procedure of Fig. 8 occurs. If an error 900 in the restoration procedure occurs in step 900, the pristine copy of the operating system files which were copied from the operating system backup area 413 to the reserved space partition area 412 in step 803 are copied back to the operating system backup area 412, thereby ensuring that a valid operating system is contained in the operating system back up area 412, before a re-set with data delete procedure is activated. In step 901 a reset with data delete procedure is activated, in which the computer entity is reset with deletion of data, which puts the computer entity into a known good state, with system data in a known good state. In step 902 after performing the reset with data deletion, the utility displays an error message on the administration web page, and on the liquid crystal display interface, to alert the user that the tape recovery has failed. In step 903, the utility prompts, via the web administration interface, the user to retry data recovery with another, different tape set.

[0036] In a case of a restore from back-up media where a known digital data storage (DDS-4) autoloader is used, where a plurality of tape data storage media are loaded into a plurality of slots in an autoloader device, the back-up media restore utility 501 should automatically load the correct back-up tapes in the correct order. Therefore, in a case where a user has replaced the tapes in a slot magazine of an autoloader in the wrong order, and so the back-up media restore utility 501 can not assume that the first tape in a set of tapes is in a first slot in a set of slots and the second tape is in the second slot etc., an algorithm comprising the back-up media restore utility checks which tape is in which slot and loads data from the tapes in the correct order.

[0037] Referring to Fig. 10 herein, there are illustrated process steps for carrying out a RESET with data preserved operation 1000. During the rebuild of the primary operating system, the computer entity runs under control of the emergency operating system. In step 1001 the emergency operating system is started, either by a failsafe BIOS, or by the installation component 1002 forcing the emergency operating system to boot from the emergency operating system boot partition 307. In step 1002, the emergency operating system successfully booting results in an automatic reset of a BIOS boot counter. In step 1003, there is displayed an "*initializing operating system rebuild\update*" message on the liquid crystal display 103. In step 1004, a primary operating system restore utility 502 is started. In step 1005, the primary operating system restore utility 502 detects that restore of the primary operating system with preserve of data is to be effected due to a "*RESET with user data deletion*" flag being read. If the flag is not set, then the reset with data preserve operation is effected. In step 1006, the primary operating system restore utility 1003 overrides the primary operating system boot partition 406 and the primary operating system system partition 403 using the content of the operating system back-up area 413 as it's source. Since the content of the operating system back-up area has been loaded with a pristine copy of the primary operating, this effectively overwrites the primary operating system system partition 403 and primary operating system boot partition 406 with the new version primary operating system which had been loaded in from the data carrier. In step 1007, the primary operating system utility 502 sets an *"system reset: restore user settings"* flag. In step 1008, it is checked whether the *"manual reset"* flag is set, and if so, then the primary operating system restore utility 502 sets a *"system reset: manual initiation"* flag and then clears the *"manual reset"* flag. In step 1010, the reboot is activated by the primary operating system restore utility 502 activating an automatic reboot to the primary operating system, from the primary operating system boot partition 406, which sets a new system identification (SID). After the system identification is set, network provisioning component 503 restores network settings and network system names from the user settings archive partition 411. Use of a new *SQLBOOT.DLL* file avoids problems due to changing the system name. Performing an automatic reboot enables network settings to be restored in step 1014. In step 1015, the "*system reset: restore user setting*" flag is checked. If the flag is set, then in step 1017 there is attempted a restore of client user account information, application configuration settings, and administration name\password from the user settings archive data stored in the user settings archive partition 411. If the archive signature is incorrect in step 1018, then the user\configuration settings should be set back to default values in step 1019 and an alert should be logged to this failure in step 1021 based upon the settings of the special flags. In step 1022 all special flags are cleared and in step 1023, the primary operating system restore utility 502 automatically reapplies any "hot fix" patches which are stored in the operating system back-up area 413.

[0038] Referring to Fig. 11 herein there is illustrated schematically process steps for a version control which checks for valid operating system version. In step 1100 the back-up media restore utility 501 checks the operating system major version number from the operating system version on the back up media. In step 1101, there is checked an operating system minor version number from the operating system version stored on the back up media. In step 1102, primary operating system version settings read from the back-up media are stored in the user settings archive partition 411, depending upon the results of steps 1100 to 1102.

[0039] The version control operates to ensure that incompatible primary operating system updates are not

applied to the computer entity. The primary operating system version numbering scheme uses a major version and a minor version number, for example in the format **XX.YY** as follows: The primary operating system major version number (XX) is incremented when a new primary operating system build has:

- major changes to user data structure such that automatic data upgrade functionality is not supported, for example moving from SQL server version 7 to version 8; or
- has hardware dependencies that are not compatible with an existing hardware type of the computer entity.

[0040] Each major version number will have a list of supported computer entity hardware types on which that operating system version will run.

[0041] A primary operating system minor version number is incremented when a new primary operating system build has any of:

- additional functionality (that is it is compatible with a major revision supported hardware type);
- has changed a base operating system to a new, but still compatible version, for example moving from Microsoft NT4 to Microsoft Windows 2000®;
- has patches for bug fixes;
- has updates to device drivers which are backwards compatible with all variants of a major revision supported hardware types;

[0042] Updates to a primary operating system which is incompatible with a hardware type of the computer entity to which loading is attempted are prevented by means of a hardware type number. The hardware type number is stored in a capacity license "raw disk" sector of the data storage device of the computer entity. This hardware type number is read in step 702. Hardware types include different types of computer entity, for example which have different data storage capacities or different application functionality. Hardware components within a particular hardware type can be changed without changing the hardware type number so long as they perform exactly the same function, that is for example changing one CD ROM reader device for another CD ROM reader device. This means that a current hardware type must be stored during a back-up operation on back-up tape device 105 to ensure that the back-up tape can only be restored onto the same type of hardware on which the back-up was created. The hardware type data read from the raw disk sector is compared with the supported hardware types of the operating systems stored on the data carrier in step 703.

[0043] By applying a version control in the restore procedure, it is ensured that the computer entity can not be downgraded in operating system to an earlier operating system version. Further, if a later version computer entity hardware replaces a previous version computer entity, then the operating system corresponding to the latest version computer entity and not overwritten by an earlier operating system version corresponding to an earlier version computer entity. For example where a computer entity using operating system version 1.0 is damaged irreparably, or stolen, and it is required to restore from a back-up data storage medium, onto a new version computer entity, where the new version computer entity is designed to operate with a later version op, e.g. version 1.1 or above, then version control prevents the new computer entity being loaded with the back-up operating system version 1.0. The operating system back-up area on the new computer entity containing a more recent operating system version, e.g. 1.0 or above, can not be overwritten by the back-up operating system version 1.0. Therefore, operating system downgrades are prohibited.

[0044] If, during a restore with data preserve operation, there is detected an earlier operating system version data, e.g. data written in back-up operating system version 1.0, but the computer entity is a new entity having a later operating system version. e.g. version 1.1 or above, then the later minor version incremented operating system stored on the operating system back-up area of the computer entity automatically upgrades the data recovered from the back-up data storage medium to the new operating system minor version upgrade. Therefore, it is always ensured that after a recovery from back-up data storage medium, the latest version operating system within the computer entity it used.

[0045] Referring to Fig. 12 herein, there is illustrated schematically a process 1200 followed for checking an operating system version stored on the back-up data storage media. The operating system stored on the back-up data storage media is only restored to the operating system back-up area partition 413, if the version stored on the back-up data storage media is an equal or greater version of operating system than is already stored on the computer entity. In step 1201, the major and minor version numbers of the operating system are read from the operating system stored on the back-up media. In step 1202, if the major version number of the primary operating system stored on the back-up media (*back-up POS major version*) is equal to the major version of the current primary operating system stored on the computer entity (*current POS major version*), then in step 1203, the minor versions are checked. In step 1203, if the minor version of the operating system stored on the back-up data storage media is less than or equal to the current primary operating system minor version stored on the computer entity (*current POS minor version*), then step 806 is skipped, so that the operating system files on the back-up data storage medium are

not restored to the operating system back up area on the computer entity, thereby avoiding a minor operating system version downgrade. If any other operating system version combination is detected, then in step 806 the operating system version stored on the back-up data storage media is restored to the operating system back-up area 413 stored on the computer entity, so that the operating system version on the computer entity matches that on the back-up data storage media.

Claims

1. A method of performing a recovery operation of an operating system for a computer entity, said computer entity comprising:

   at least one data processor; and

   at least one data storage device, wherein said data storage device is configured into a plurality of partition areas;

   said method comprising the steps of:

   copying a back-up operating system from a back-up source onto an operating system back-up area partition which is not used for direct running of an operating system by said computer entity;

   copying a user settings data from said back-up source to a user settings archive partition area of said data storage device; and

   resetting said computer entity.

2. The method as claimed in claim 1, further comprising the step of:

   prior to said step of copying said back-up operating system to said operating system back-up area partition, copying a content of said operating system back up area partition into a reserved space partition area of said data storage device.

3. The method as claimed in claim 1, further comprising the step of:

   checking a version of said back-up operating system stored on a back-up data storage media; and

   comparing said operating system version, with a hardware of said computer entity.

4. The method as claimed in claim 1, further comprising the step of:

   copying said back-up operating system from said operating system back-up partition area to a primary operating system partition area of said data storage device, wherein said step of resetting said computer entity comprises rebooting from said back-up copy operating system copied to said primary operating system partition, and said user settings data copied from said user settings archive partition.

5. The method as claimed in any one of claims 1 to 4, further comprising the step of:

   copying user data from said back-up source to one or more data partitions of said data storage device, said secondary data partition area being a data partition area for storage of data.

6. The method as claimed in any one of claims 1 to 5, wherein said step of resetting said computer entity comprises the steps of:

   forcing said computer entity to boot from an emergency operating system stored on an emergency operating system partition area of said data storage device;

   overwriting a content of said primary operating system partition with said back-up operating system stored in said operating system back-up area partition; and

   restoring client and application configuration settings from said user settings archive partition area.

7. The method as claimed in claim 3, wherein said step of checking a version of said back-up operating system with a hardware of said computer entity comprises:

   reading a list of supported hardware types from said operating system stored on said back-up media;

   comparing said read list of supported hardware types with a current hardware type data stored on said computer entity;

   if said current hardware type data stored on said computer entity is incompatible with said read list of supported hardware types, generating an error message.

8. The method as claimed in claim 1, wherein said step

of resetting said computer entity comprises:

resetting said computer entity, including deleting application and user configuration setting data; and

restoring said user configuration and setting data from said user settings archive partition area.

9. The method as claimed in claim 1, further comprising the step of:

if an error occurs in said recovery operation, storing an event data describing at least one event of said restore operation.

10. The method as claimed in claim 1, further comprising the step of:

if an error occurs in said recovery operation, restoring a primary operating system to a primary operating system partition area of said data storage device reserved for use by said primary operating system, from a copy of said primary operating system temporarily stored in a reserved space partition of said data storage device.

11. The method as claimed in claim 10, wherein said step of resetting said computer entity comprises deleting user settings data.

12. The method as claimed in claim 1, further comprising the steps of:

restoring said operating system back-up area partition of said data storage device;

restoring said user settings archive partition area of said data storage device; and

restoring at least one user data partition area.

13. A method of storing a back-up operating system of a computer entity to a back-up media, said computer entity comprising a pristine copy of an operating system stored in an operating system back-up area data partition of a data storage device, and a primary operating system stored in a primary operating system partition area of said data storage device;
said method comprising:

copying a plurality of operating system files in a pristine manufactured state from said operating system back up area data partition onto a back-up media; and

copying a set of configuration settings from a user settings archive partition area of said data storage device to said back-up media.

14. The back-up method as claimed in claim 13, further comprising the step of:

copying user data from a data partition of said data storage device to said back-up media.

15. The back-up method as claimed in claim 13 or 14, further comprising the step of:

copying user data from a secondary data partition of said data storage device onto said back-up media.

16. The back-up method as claimed in claim 13, further comprising the step of:

copying data uniquely identifying said computer entity to said back-up media.

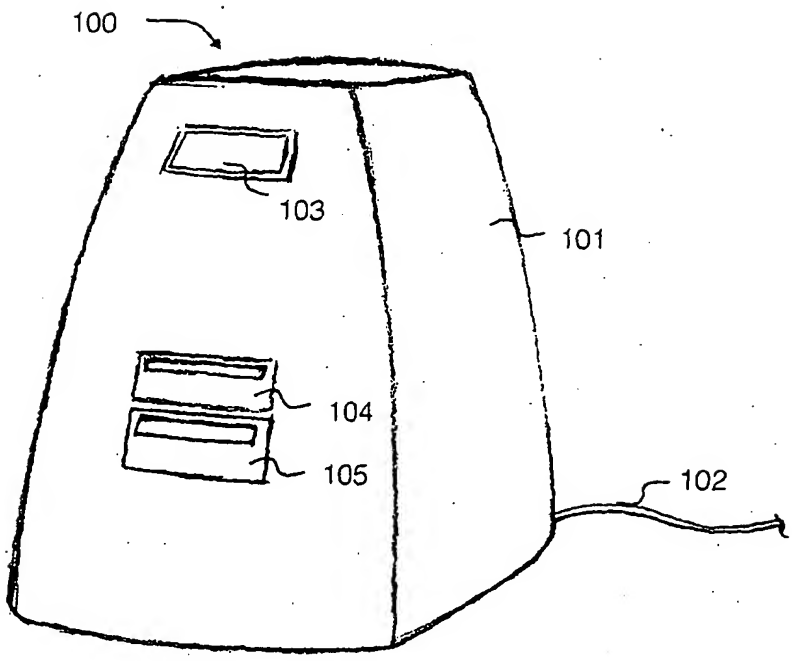

Fig. 1

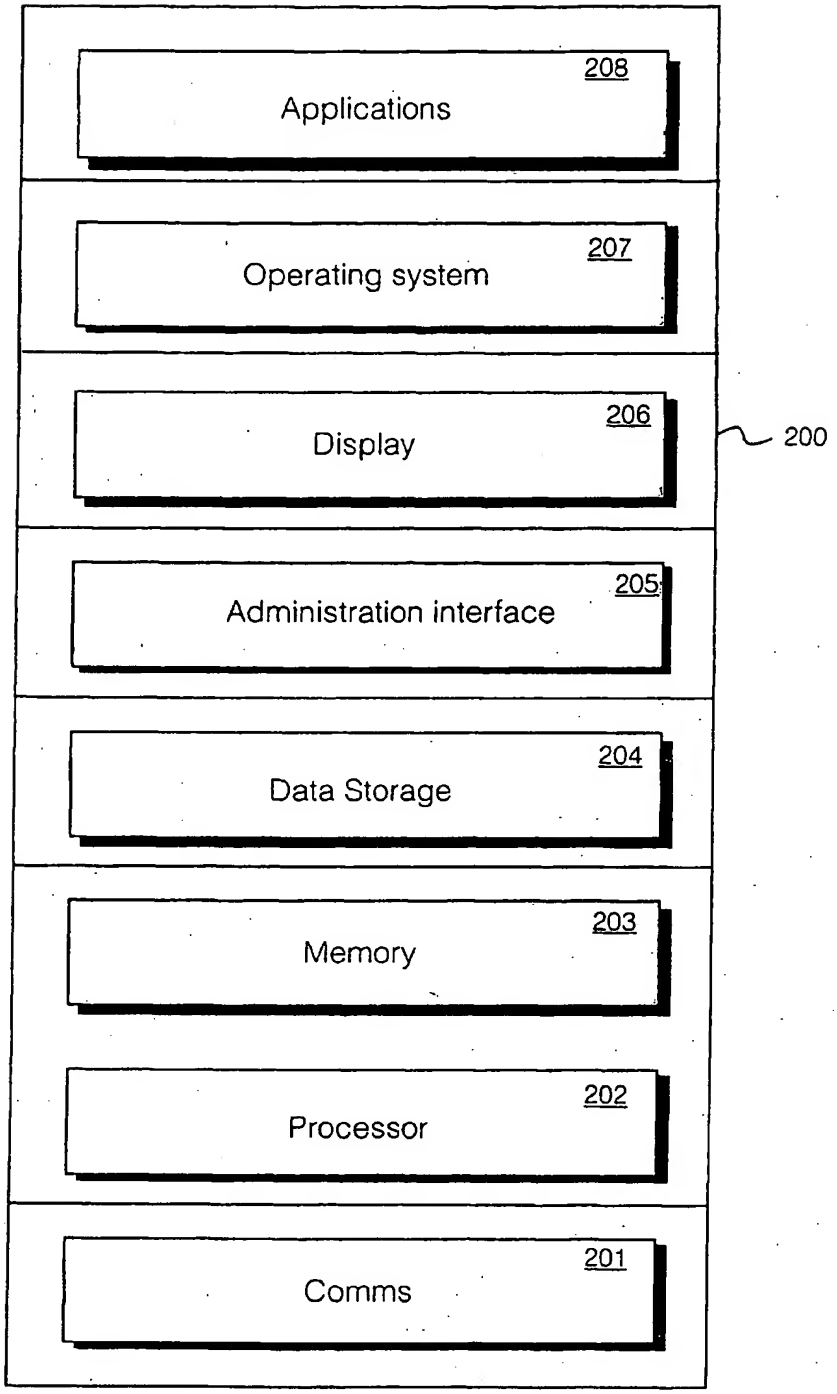
208
Applications
207
Operating system
206
Display
200
205
Administration interface
204
Data Storage
203
Memory
202
Processor
201
Comms

Fig. 2

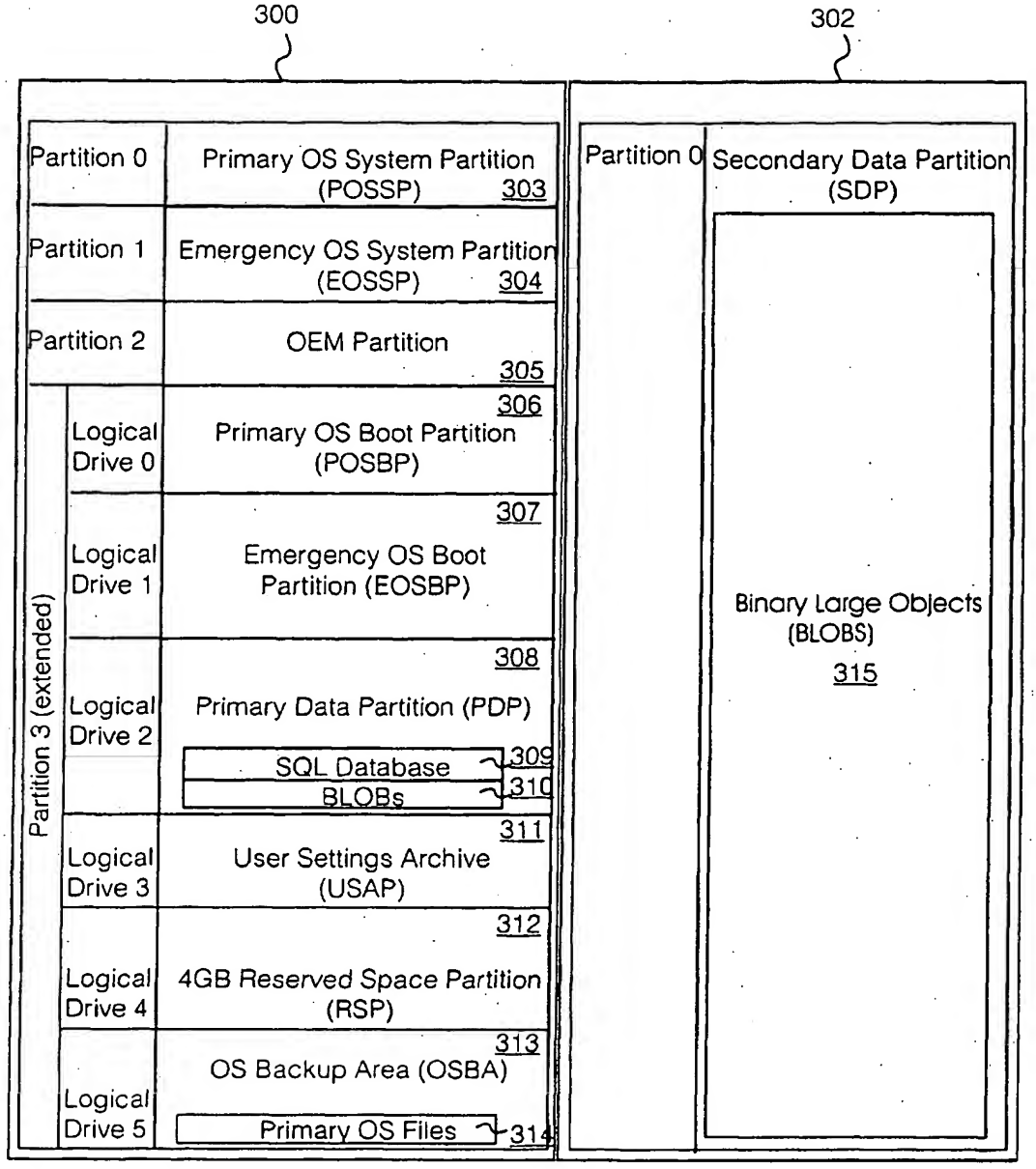
300
302
Partition 0
Primary OS System Partition (POSSP) 303
Partition 1
Emergency OS System Partition (EOSSP) 304
Partition 2
OEM Partition 305
Partition 3 (extended)
Logical Drive 0
306
Primary OS Boot Partition (POSBP)
Logical Drive 1
307
Emergency OS Boot Partition (EOSBP)
Logical Drive 2
308
Primary Data Partition (PDP)
SQL Database 309
BLOBs 310
Logical Drive 3
311
User Settings Archive (USAP)
Logical Drive 4
312
4GB Reserved Space Partition (RSP)
Logical Drive 5
313
OS Backup Area (OSBA)
Primary OS Files 314
Partition 0
Secondary Data Partition (SDP)
Binary Large Objects (BLOBS)
315

Fig. 3

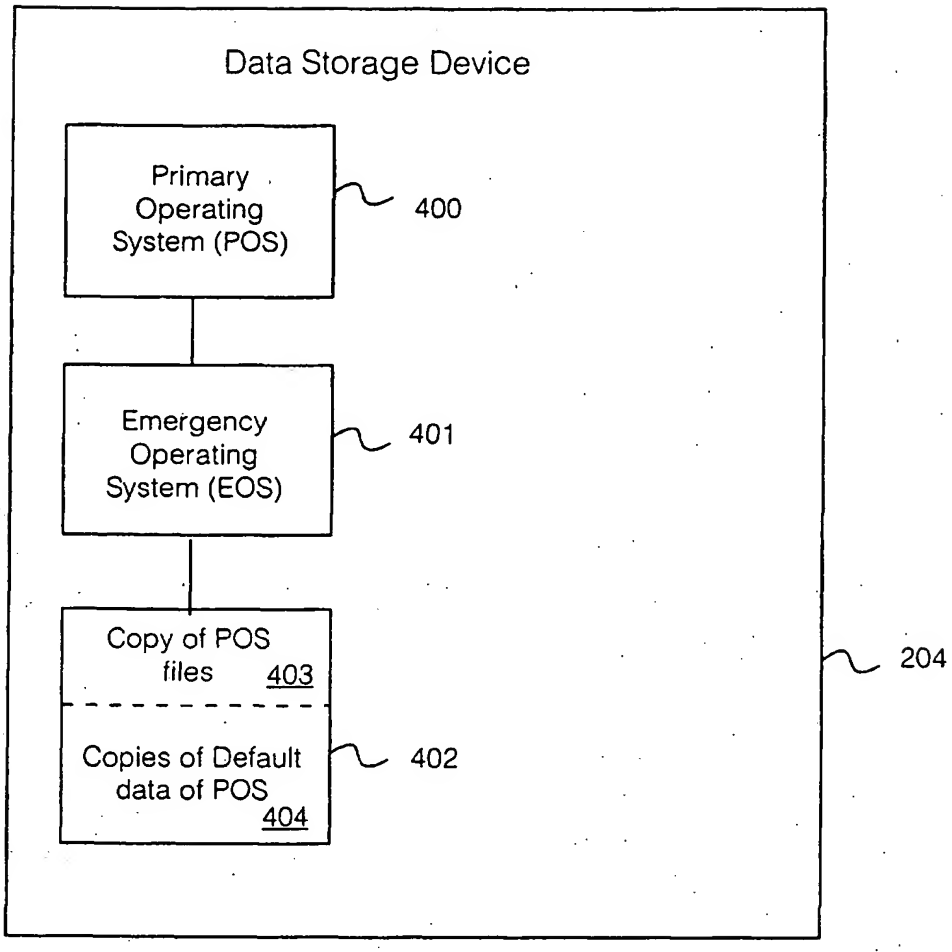
Data Storage Device
Primary Operating System (POS)
400
Emergency Operating System (EOS)
401
Copy of POS files
403
Copies of Default data of POS
404
402
204

Fig. 4

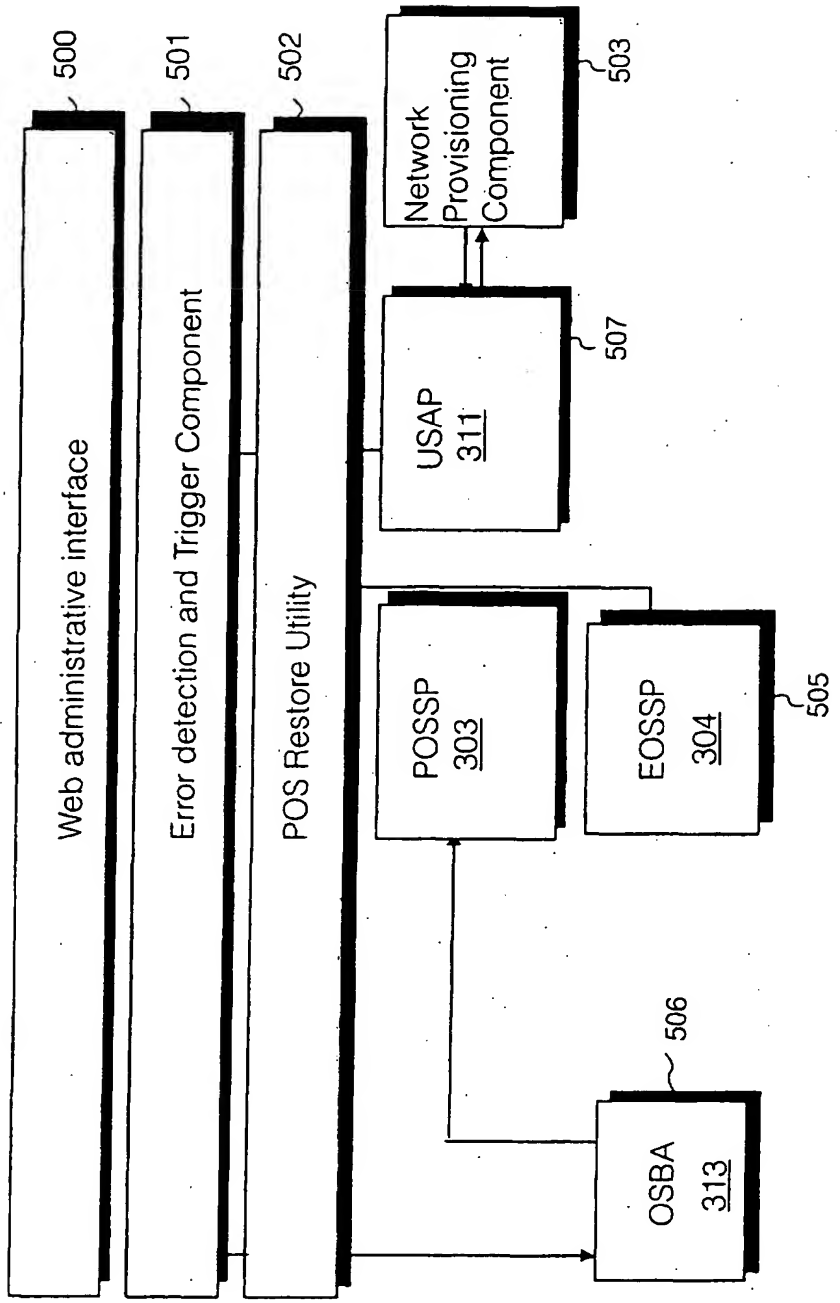
500
501
502
503
Web administrative interface
Error detection and Trigger Component
POS Restore Utility
Network Provisioning Component
USAP 311
507
POSSP 303
EOSSP 304
505
506
OSBA 313

Fig. 5

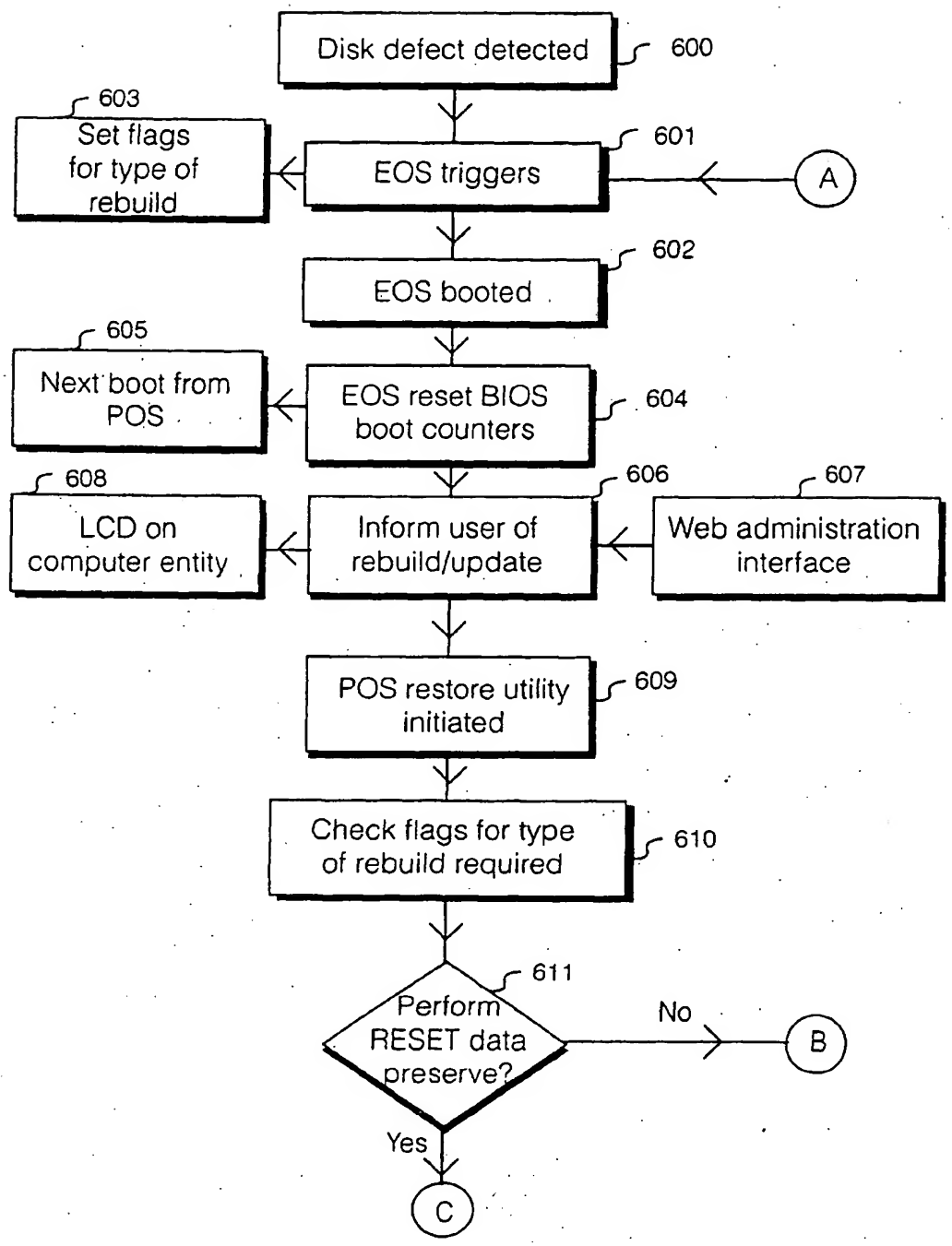
Disk defect detected
600
603
Set flags for type of rebuild
601
EOS triggers
A
602
EOS booted
605
Next boot from POS
EOS reset BIOS boot counters
604
608
LCD on computer entity
606
Inform user of rebuild/update
607
Web administration interface
POS restore utility initiated
609
Check flags for type of rebuild required
610
611
Perform RESET data preserve?
No
B
Yes
C

Fig. 6

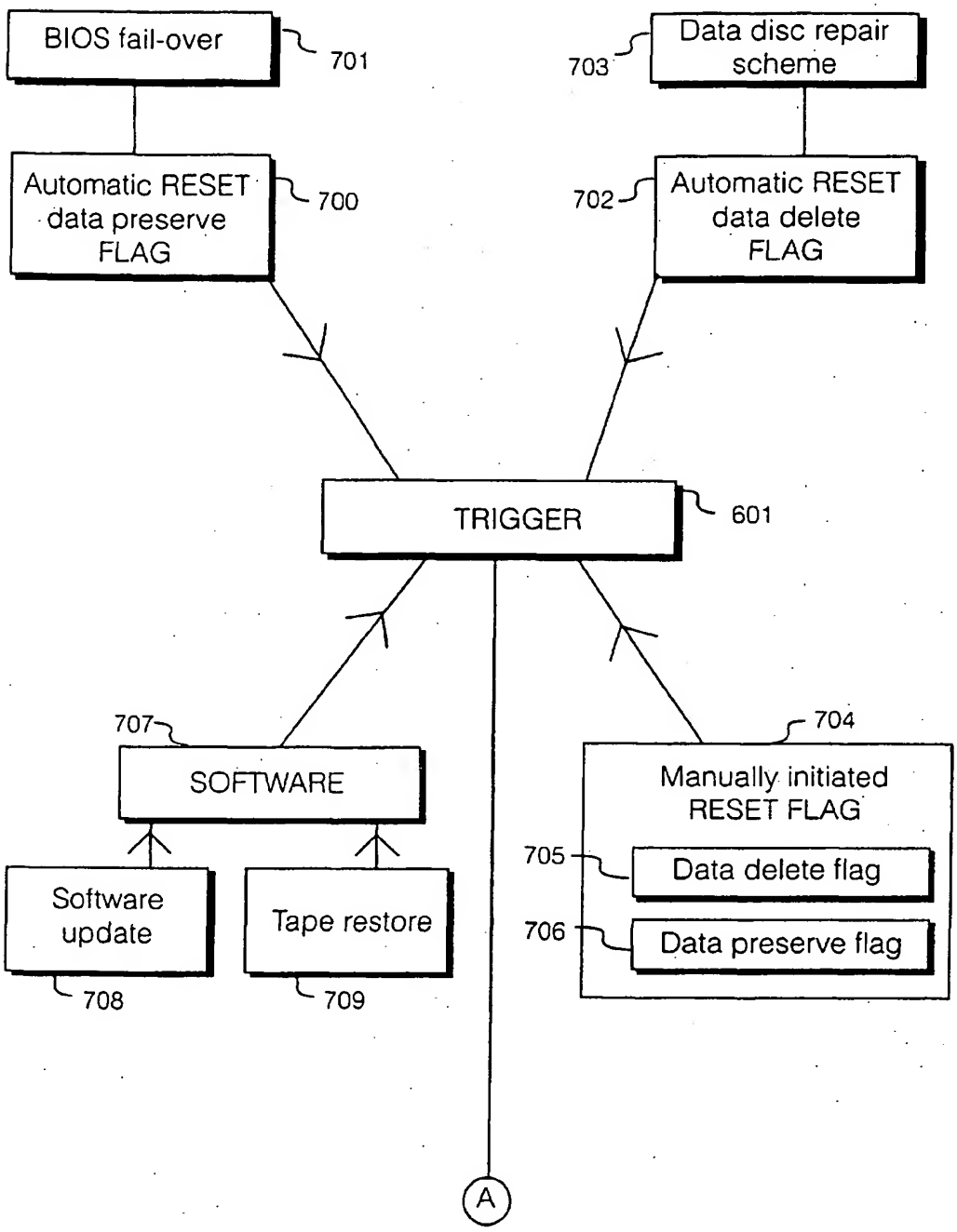
BIOS fail-over
701
Data disc repair scheme
703
Automatic RESET data preserve FLAG
700
Automatic RESET data delete FLAG
702
TRIGGER
601
707
SOFTWARE
704
Manually initiated RESET FLAG
705
Data delete flag
706
Data preserve flag
Software update
708
Tape restore
709
A

Fig. 7

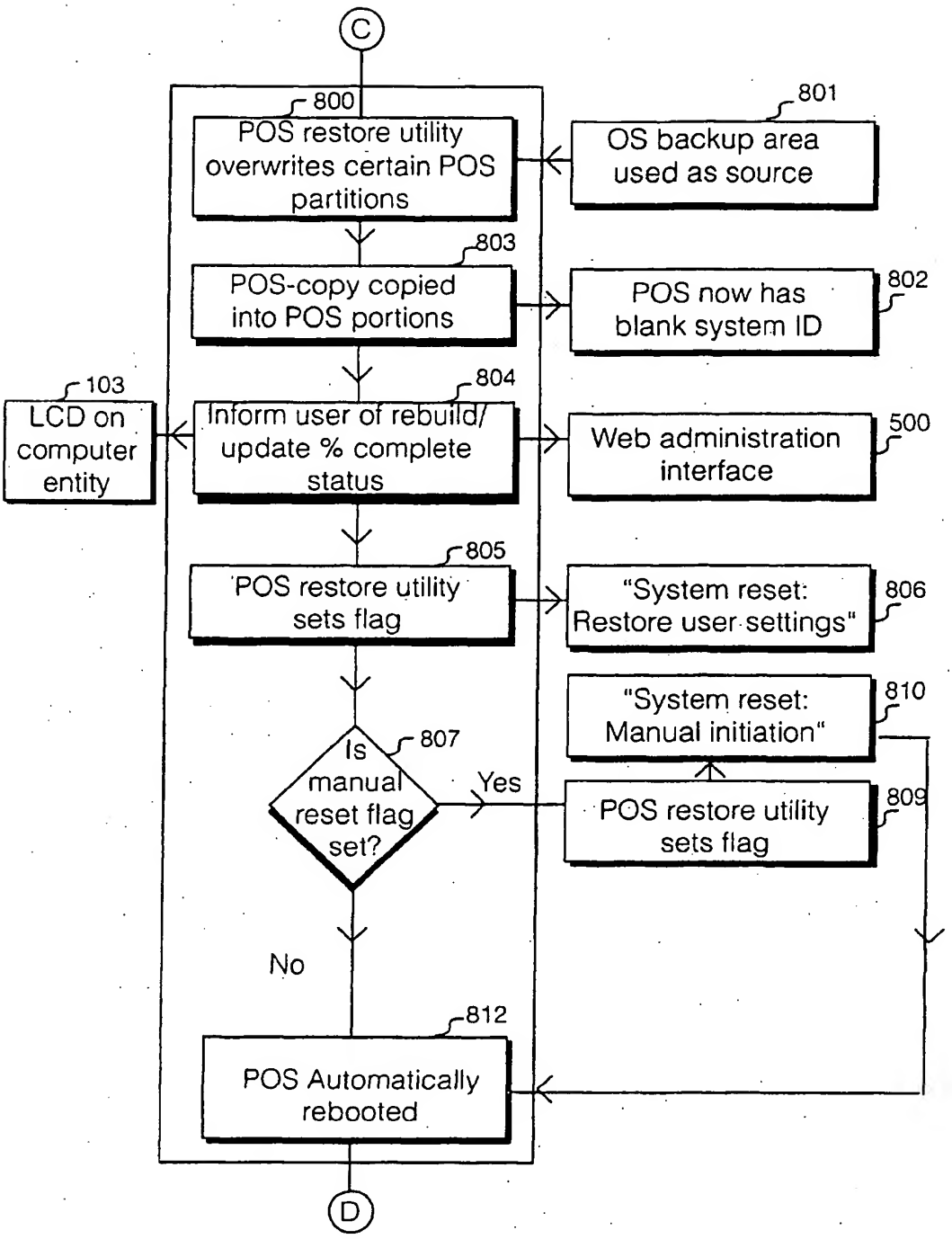
C
800
POS restore utility overwrites certain POS partitions
801
OS backup area used as source
803
POS-copy copied into POS portions
802
POS now has blank system ID
103
LCD on computer entity
804
Inform user of rebuild/ update % complete status
500
Web administration interface
805
POS restore utility sets flag
"System reset: Restore user settings"
806
"System reset: Manual initiation"
810
807
Is manual reset flag set?
Yes
POS restore utility sets flag
809
No
812
POS Automatically rebooted
D

Fig. 8

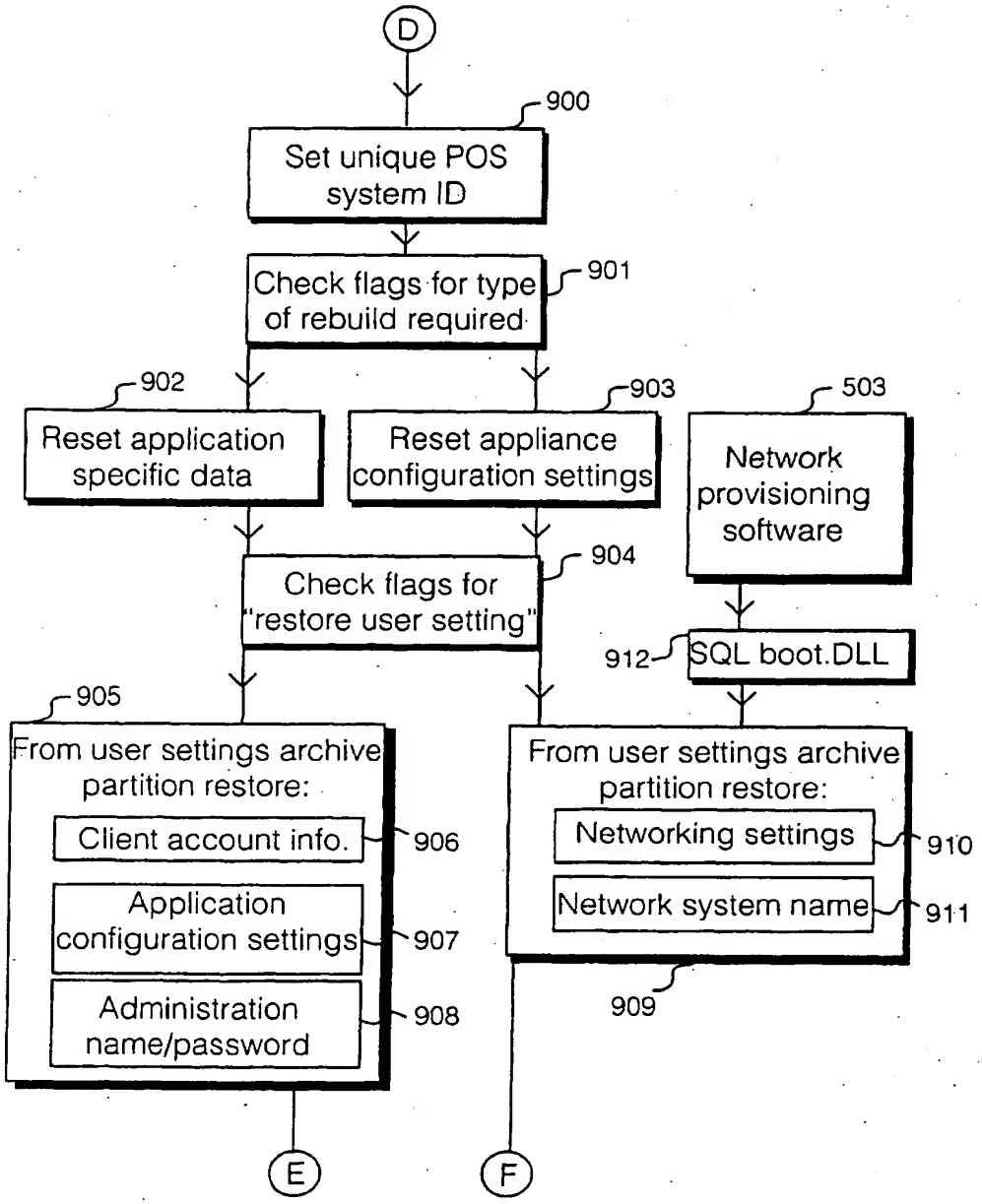
D
900
Set unique POS system ID
Check flags for type of rebuild required
901
902
903
503
Reset application specific data
Reset appliance configuration settings
Network provisioning software
Check flags for "restore user setting"
904
912
SQL boot.DLL
905
From user settings archive partition restore:
Client account info.
906
Application configuration settings
907
Administration name/password
908
From user settings archive partition restore:
Networking settings
910
Network system name
911
909
E
F

Fig. 9

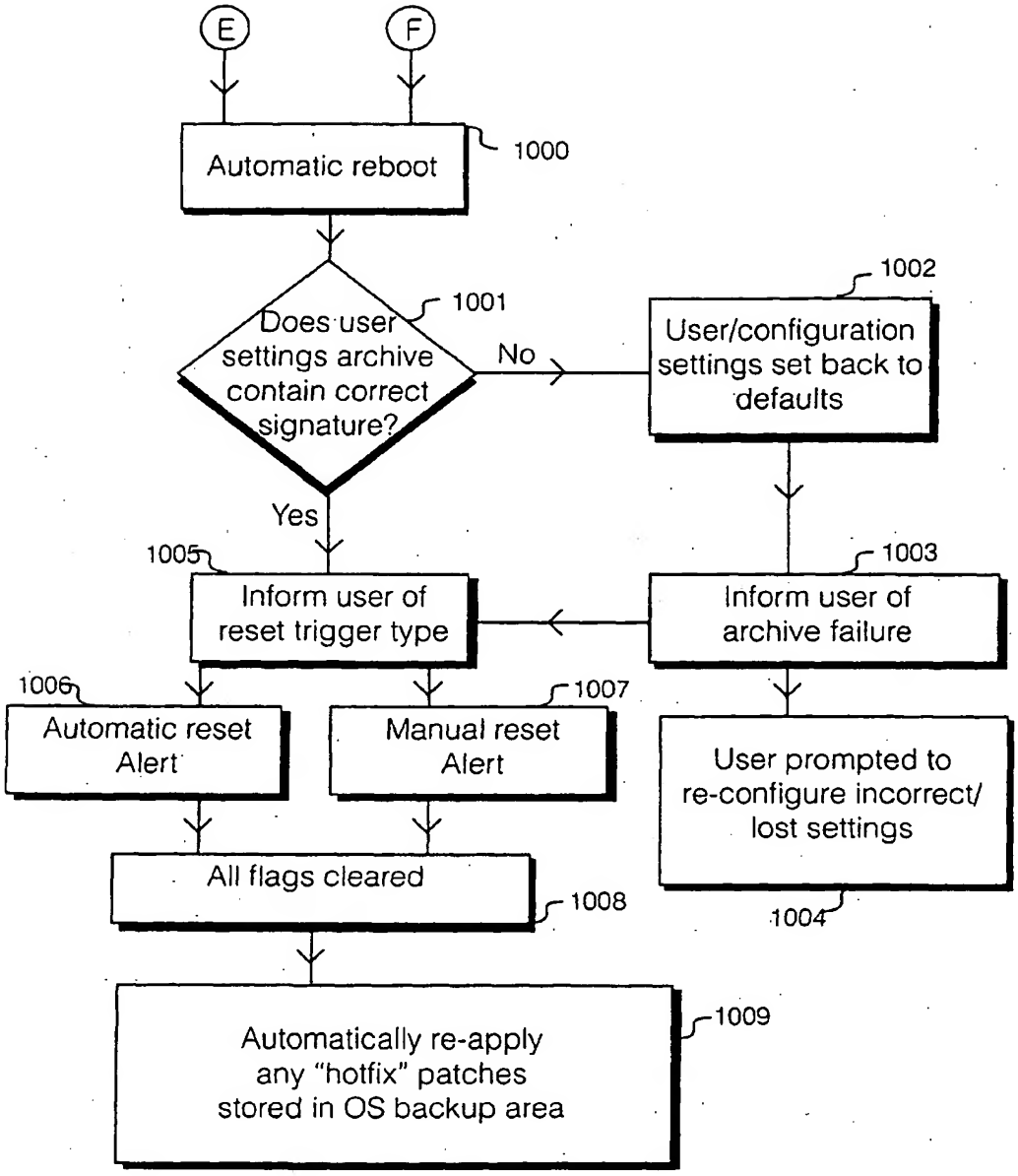
E
F
Automatic reboot
1000
Does user settings archive contain correct signature?
1001
No
User/configuration settings set back to defaults
1002
Yes
1005
Inform user of reset trigger type
1003
Inform user of archive failure
1006
Automatic reset Alert
1007
Manual reset Alert
User prompted to re-configure incorrect/ lost settings
1004
All flags cleared
1008
Automatically re-apply any "hotfix" patches stored in OS backup area
1009

Fig. 10

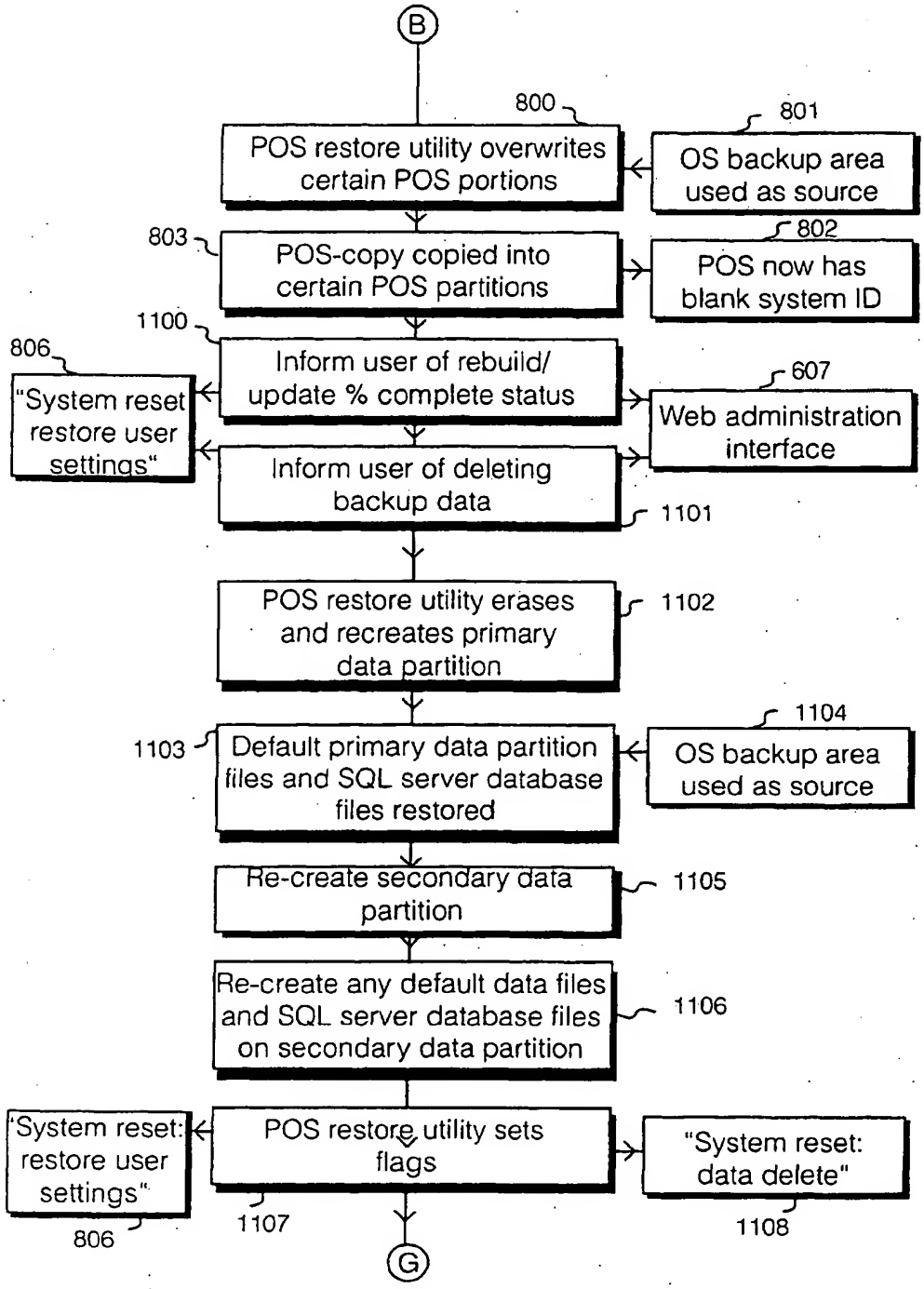
B
800
POS restore utility overwrites certain POS portions
801
OS backup area used as source
803
POS-copy copied into certain POS partitions
802
POS now has blank system ID
1100
Inform user of rebuild/ update % complete status
806
"System reset restore user settings"
607
Web administration interface
Inform user of deleting backup data
1101
POS restore utility erases and recreates primary data partition
1102
1104
1103
Default primary data partition files and SQL server database files restored
OS backup area used as source
Re-create secondary data partition
1105
Re-create any default data files and SQL server database files on secondary data partition
1106
"System reset: restore user settings"
806
POS restore utility sets flags
1107
"System reset: data delete"
1108
G

Fig. 11

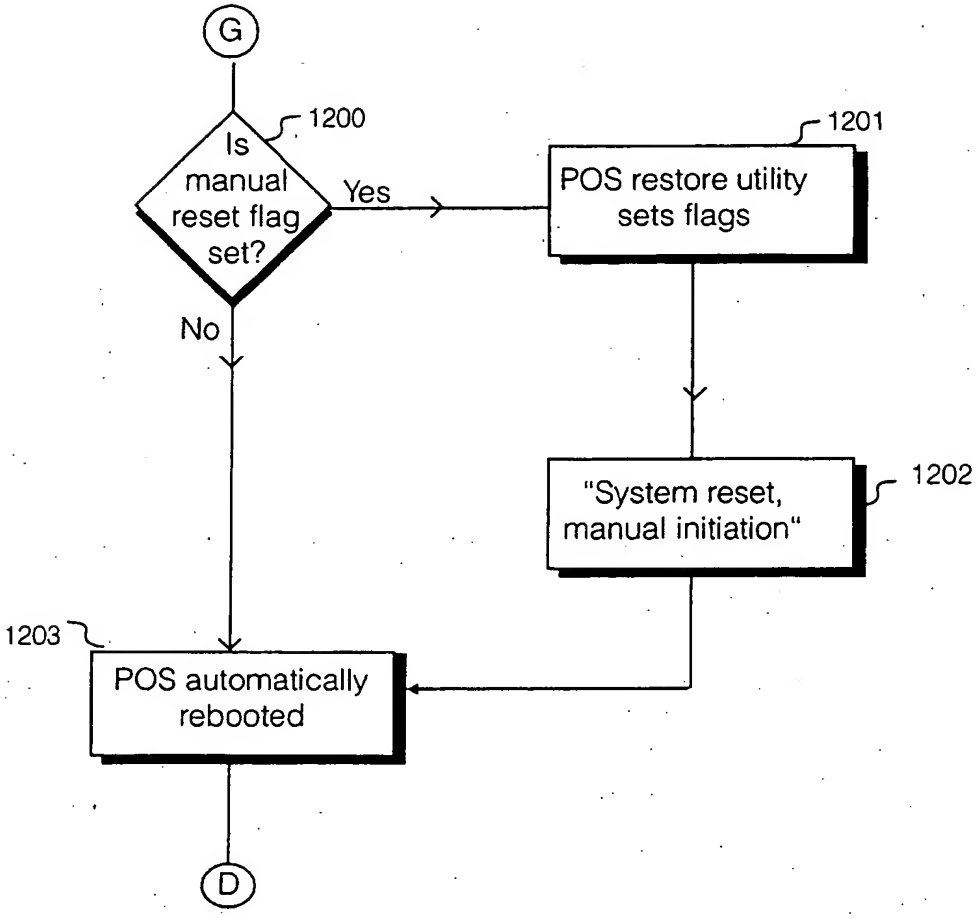
G
1200
Is manual reset flag set?
Yes
No
1201
POS restore utility sets flags
"System reset, manual initiation"
1202
1203
POS automatically rebooted
D

Fig. 12

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 8840

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	GB 2 336 921 A (IBM) 3 November 1999 (1999-11-03) * the whole document *	1,13	G06F11/14
A	EP 0 917 060 A (IOMEGA CORPORATION) 19 May 1999 (1999-05-19) * the whole document *	1,13	
A	EP 0 898 225 A (SONY CORPORATOIN) 24 February 1999 (1999-02-24) * the whole document *	1,13	
A	EP 0 978 785 A (HEWLETT PACKARD CO) 9 February 2000 (2000-02-09) * the whole document *	1,13	
A	US 5 269 022 A (SHINJO KAZUYA ET AL) 7 December 1993 (1993-12-07) * the whole document *	1,13	
A	WO 95 22794 A (APPLE COMPUTER ;YEN JOHN (US)) 24 August 1995 (1995-08-24) * the whole document *	1,13	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F
A	GB 2 346 719 A (DELL USA LP) 16 August 2000 (2000-08-16) * abstract * * page 6, line 26 - page 7, line 11 * * page 10, line 8 - line 26 *	1,13	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	30 March 2001	Absalom, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 00 30 8840

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

30-03-2001

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2336921 A	03-11-1999	US 6167494 A	26-12-2000
EP 917060 A	19-05-1999	US 6170055 B	02-01-2001
		AU 1368499 A	24-05-1999
		FR 2772947 A	25-06-1999
		GB 2332076 A	09-06-1999
		WO 9923561 A	14-05-1999
EP 898225 A	24-02-1999	WO 9834169 A	06-08-1998
EP 0978785 A	09-02-2000	GB 2344441 A	07-06-2000
		WO 0008561 A	17-02-2000
US 5269022 A	07-12-1993	JP 2772103 B	02-07-1998
WO 9522794 A	24-08-1995	AU 1876895 A	04-09-1995
GB 2346719 A	16-08-2000	AU 6314399 A	27-07-2000
		BR 9905743 A	12-09-2000
		CN 1257245 A	21-06-2000
		DE 19960524 A	03-08-2000
		FR 2788356 A	13-07-2000
		JP 2000181772 A	30-06-2000

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82